



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,265	08/01/2001	Warwick Ford		8690
Warwick Ford 6 Ellery Square Cambridge, MA 02138				
7590 05/25/2007			EXAMINER HENNING, MATTHEW T	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 05/25/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/921,265

Applicant(s)

FORD, WARWICK

Examiner

Matthew T. Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 January 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 and 10-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 and 10-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Art Unit: 2131

This action is in response to the communication filed on 1/22/2007.

DETAILED ACTION

In view of the Appeal Brief filed on 1/22/2007, PROSECUTION IS HEREBY
REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following
two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37
CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an
appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee
can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have
been increased since they were previously paid, then appellant must pay the difference between
the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing
below:

Claims 1-8, and 10-19 have been examined and claim 9 has been cancelled.

All objections and rejections not set forth below have been withdrawn.

1 *Response to Arguments*

2 Applicant's arguments, see Appeal Brief, filed 1/22/2007, with respect to the rejection(s)
3 of the claim(s) in view of Fielder et al. have been fully considered and are persuasive. Therefore,
4 the rejection has been withdrawn. However, upon further consideration, a new ground(s) of
5 rejection is made in view of Mills, as presented below.

6 *Claim Objections*

7 Claim 4 is objected to because of the following informalities: Claim 4 recites the
8 limitation "the user device" which lacks antecedent basis in the claim. For purposes of searching
9 prior art the examiner will assume the limitation was meant to read "a user device". Appropriate
10 correction is required.

11
12 *Claim Rejections - 35 USC § 103*

13 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
14 obviousness rejections set forth in this Office action:

15 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
16 section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
17 such that the subject matter as a whole would have been obvious at the time the invention was made to a person
18 having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the
19 manner in which the invention was made.

20
21 Claims 1, 5-8, 10-11, and 13-19 are rejected under 35 U.S.C. 103(a) as being
22 unpatentable over Mills (US Patent Number ,991,405), and further in view of Lamport, Leslie
23 (Password Authentication with Insecure Communication) hereinafter referred to as Lamport.

24 Regarding claims 1, 18, and 19, Mills disclosed a method for validating a client device
25 (Cellular Phone) by a server device (HLR), said method comprising the steps of: generating a
26 shared unpredictable secret (See Mills Fig. 1 and Col. 5 Paragraph 3 "update the encryption

Art Unit: 2131

key”); storing the shared unpredictable secret in the client device and in the server device (See Mills Fig. 1 and Col. 5 Paragraph 3); requiring the client device to authenticate itself to the server device as a precondition to the server device validating the client device (See Mills Col. 4 Lines 34-50); and replacing the shared unpredictable secret by a new shared unpredictable secret when the server device validates the client device (See Mills Fig. 1 and Col. 7 Paragraph 3), wherein: the server device sends update data to the client device (See Mills Fig. 1 Message 10 SSD and Col. 6 Lines 35-58); the client device applies the update data to the shared unpredictable secret to generate a new secret (See Mills Col. 7 Paragraph 3); and the client device replaces the shared unpredictable secret with the new secret (See Mills Col. 7 Paragraph 3), but Mills fails to disclose the specifics of the authentication, including the client proving the holding of a correct secret. Mills does disclose use of the new secret (new shared encryption key) in authentication (See Mills Col. 7 Paragraph 3).

Lamport teaches a method of authentication in which for some fixed word ‘x’, a one-way function $F(x)$ is applied a predetermined number of times to ‘x’, which is then sent to a system to prove authenticity through knowledge of ‘x’, and the system verifies the received $F(x)$ in order to authenticate the user (See Lamport page 771 Col. 1 – Col. 2 Paragraph 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lamport in the phone system of Mills by utilizing the one-time password scheme in order to authenticate the phone as required by Mills. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to provide a robust manner of authenticating the cellular phone to the HLR. It further would have been obvious in this combination to use the encryption key to encrypt and

Art Unit: 2131

1 decrypt the communications between the cellular telephone and HLR, including the generated
2 password. This would have been obvious because the ordinary person skilled in the art would
3 have been motivated to protect the communications from being intercepted during transmission.

4 Regarding claim 5, Mills and Lamport disclosed that the shared unpredictable secret
5 (New Encryption Key) is generated by a generator from a group comprising a random number
6 generator and a pseudo-random number generator (See Mills Col. 7 Paragraph 3).

7 Regarding claim 6, Mills and Lamport disclosed that the shared unpredictable secret
8 comprises an unpredictable component and a fixed component (See Mills Col. 7 Paragraph 3).

9 Regarding claim 7, Mills and Lamport disclosed that a plurality of client devices desire to
10 be validated by the server device; and each client device has a unique unpredictable secret that it
11 shares with the server device (See Mills Abstract).

12 Regarding claim 8, Mills and Lamport disclosed that following a validation of the client
13 device, the server device discards the shared unpredictable secret and stores within the server
14 device the new shared unpredictable secret that can be generated by applying the update data to
15 the shared unpredictable secret (See Mills Col. 7 Paragraph 3).

16 Regarding claim 10, Mills and Lamport disclosed that the server device generates the
17 update data using a generator from a group comprising a random number generator and a
18 pseudo-random number generator (See Mills Col. 6 Paragraph 2); and the step of applying the
19 update data to the shared unpredictable secret comprises computing a one-way function of the
20 combination of the shared unpredictable secret and the update data (See Mills Col. 7 Paragraph
21 3).

1 Regarding claim 11, Mills and Lamport disclosed that the client device sends
2 acknowledgement data to the server device to confirm that the client device has replaced the
3 shared unpredictable secret with the new secret (See Mills Col. 7 Paragraph 3).

4 Regarding claim 13, Mills and Lamport disclosed that the client device sends to the
5 server device proof data demonstrating that the client device holds the correct secret (See the
6 rejection of claim 1 above and Lamport Page 771 Col. 1); and the server device is adapted to
7 accept from the client device any proof data that are generated from a secret that is newer than
8 the secret for which the most recent acknowledgment data have been received by the server
9 device (See the rejection of claim 1 above and Lamport Page 771 Col. 1).

10 Regarding claim 14 and 15, Mills and Lamport disclosed that the client device sends to
11 the server device both the acknowledgment data and proof data derived from the new secret (See
12 the rejection of claim 1 above).

13 Regarding claim 16, Mills and Lamport disclosed that the client device presents proof
14 data to the server device, wherein the proof data are derived from the shared unpredictable secret
15 using a proof data generation algorithm, and the proof data do not divulge the shared
16 unpredictable secret; the server device checks the proof data by using a proof data generation
17 algorithm consistent with the proof data generation algorithm used by the client device; and
18 when the server device determines that the proof data presented by the client device were not
19 generated from the shared unpredictable secret that is stored in both the client device and in the
20 server device, the server device does not validate the client device (See the rejection of claim 1
21 above and Lamport Page 771 Col. 1).

Art Unit: 2131

1 Regarding claim 17, Mills and Lamport disclosed that the proof data generation
2 algorithm is a one way function (See Lamport Page 771 Col. 1).

3 Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mills and
4 Lamport as applied to claim 1 above, and further in view of Sheymov et al. (Patent Application
5 Publication 2001/0048745) hereinafter referred to as Sheymov.

6 Mills and Lamport disclosed updating a shared unpredictable secret (See the rejection of
7 claim 1 above), but failed to disclose how the initial shared unpredictable secret was acquired, or
8 specifically that an initial shared unpredictable secret is determined in the client device and in the
9 server device during a registration step that occurs prior to a log-in step, or that the registration
10 step entails more checking of authentication data presented by the client device than does the
11 log-in step, or that during the registration step, the client device is required to make a payment to
12 a user device.

13 Sheymov teaches that at the time of purchase, a user may be required to respond to
14 screening data in order to enhance security of initialization, and that during the initialization an
15 encryption key could be assigned to the phone (See Sheymov Paragraph 0027).

16 It would have been obvious to the ordinary person skilled in the art at the time of
17 invention to employ the teachings of Sheymov in the phone system of Mills and Lamport by
18 having a user respond to screening data at the time of purchase, and that the initial encryption
19 key be stored in the phone and server during initialization of the phone. This would have been
20 obvious because the ordinary person skilled in the art at the time of invention would have been
21 motivated to provide the phone and server with initial encryption keys, as well as ensure the
22 security of the initialization.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mills and Lamport as applied to claim 11 above, and further in view of Brinkmeyer et al. (US Patent Number 5,940,007) hereinafter referred to as Brinkmeyer.

Mills and Lamport disclosed receiving acknowledgement data from the client device which validates the client device (See Mills Col. 7 Paragraph 3), but failed to disclose the server discarding the shared predictable secret and storing the new shared unpredictable secret in response to receiving the acknowledgment data.

Brinkmeyer teaches that in a system for updating keys, in order to prevent the situation where the key is updated in only one two devices, a first device should store the key and send an acknowledgement to the second device, which will erase the previous key and replace it with the new key only upon receipt of the acknowledgment (See Brinkmeyer Col. 7 Paragraphs 2-3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Brinkmeyer in the key updating system of Mills and Lamport by the HLR erasing the previous key and replacing it with the new key only upon receipt of the acknowledgment from the cellular phone. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent the situation where the HLR updated the key but the cellular telephone did not replace the key.

Conclusion

Claims 1-8, and 10-19 have been rejected and claim 9 has been cancelled.

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

Art Unit: 2131

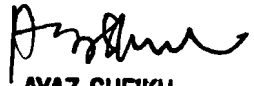
1 MONTHS of the mailing date of this final action and the advisory action is not mailed until after
2 the end of the THREE-MONTH shortened statutory period, then the shortened statutory period
3 will expire on the date the advisory action is mailed, and any extension fee pursuant to 37
4 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,
5 however, will the statutory period for reply expire later than SIX MONTHS from the mailing
6 date of this final action.

7 Any inquiry concerning this communication or earlier communications from the
8 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.
9 The examiner can normally be reached on M-F 8-4.

10 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
11 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
12 organization where this application or proceeding is assigned is 571-273-8300.

13 Information regarding the status of an application may be obtained from the Patent
14 Application Information Retrieval (PAIR) system. Status information for published applications
15 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
16 applications is available through Private PAIR only. For more information about the PAIR
17 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
18 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

19
20
21
22
23 /Matthew Henning/
24 Patent Examiner
25 Art Unit 2131
26 5/17/2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100